UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION

IN RE FOUR APPLICATIONS FOR SEARCH WARRANTS SEEKING INFORMATION ASSOCIATED WITH PARTICULAR CELLULAR TOWERS A/K/A TOWER-DUMP WARRANTS

CRIMINAL NO. 3:25-CR-38-CWR-ASH

ORDER

On February 21, 2025, the Court declined to issue four search warrants for location-and-time based cell-tower data, also known as tower-dump or tower-extraction warrants. Order [6]. The Government obtained an extension and later a stay of its deadline to seek review of that order. Orders [9], [13], [15]. The current stay expires July 21, 2025.

The matter is now before the Court on three new applications, based on some of the same underlying facts as before,[1] for tower-dump or tower-extraction search warrants. The new applications seek to obtain from three of the original four cellular service providers a list of phone numbers and identifiers for cellular devices that connected to cell towers covering six locations during specific windows of time ranging from ten to thirty minutes for each location.[2] The time windows and locations correspond to crimes the Government suspects were committed by members of a violent street gang. While the affidavit in support of the new applications somewhat narrows the scope of data sought, the Court still finds they run afoul of the Fifth Circuit's decision in *United States v. Smith*, 110 F.4th 817, 820 (5th Cir. 2024), in which the

[1] Given the commonality, the Court directs the Clerk to file the three new applications and affidavit and this order in Case No. 3:25-CR-38-CWR-ASH. The applications and affidavit will be filed under seal due to the connection to an ongoing criminal investigation.

[2] The applications also seek information for communications beginning before or ending after the specified intervals if any portion of the communications occurred within the requested windows of time.

court concluded that geofence warrants are per se "unconstitutional under the Fourth Amendment." Like the previous applications and the warrant in *Smith*, the proposed tower-dump search warrants cannot be issued consistent with the Fourth Amendment. For the reasons explained below and in its previous Order [6], the Court therefore declines to issue the warrants.

I. Background

According to the affidavit of an FBI Special Agent supporting the search-warrant applications, law enforcement suspects the involvement of various members of a violent street gang in several violent crimes, which law enforcement believe are interconnected. *See generally* Aff.

The Government has asked the Court to authorize the collection of certain cell-site location information (CSLI) data from every user of a cellular device that connected to any of the cell towers providing service to six locations tied to those incidents.[3] It proposes to provide that data to the FBI's Cellular Analysis Survey Team (CAST), "which will use analytical tools to identify . . . devices that appear in two or more of the tower locations . . . ; this information will then be provided to the investigative team." Aff. ¶ 69.[4] The FBI Special Agent says that "[b]ecause of the distinct times and locations listed in [the applications], it is unlikely that anyone other than individuals involved in [the subject] criminal activity would be at more than

[3] "When a device connects to a cell tower, it creates a time-stamped record generally called cell-site location information ('CSLI')." Aff. ¶ 54. "CSLI typically contains device communications that took place over the cellular network and includes the date, time, and duration of the connection, type of transaction (e.g., phone call, SMS text message, data session), calling party, called party, and the cell tower and sector on which the transaction took place." *Id.* ¶ 55.

[4] "[C]ellular service providers maintain antenna towers ('cell towers') that serve and provide cellular service to devices that are within range of the tower[s'] signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data." Aff. ¶ 48.

one of these locations during the time period of these events." *Id.* ¶ 52. As for data from devices that appear in only one of the tower locations, that information "will be retained by the FBI's Cellular Analysis Survey Team and will not be accessed by the investigative team absent further order of the court." *Id.* at Attachment B.II.

For each cell tower providing service to the described locations,[5] the Government seeks

> records and other information (not including the contents of communications) about all communications made using the cellular tower(s) . . . during the corresponding timeframe(s) listed . . . , including records that identify:
>
> a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower ("the locally served wireless device") that registered with the cell tower . . . ;
>
> b. for each communication, the "sector(s)" (i.e. the face(s) of the tower(s)) that received a radio signal from the locally served wireless device;
>
> c. the date, time, and duration of each communication; and
>
> d. the type of communication transmitted through the tower (such as phone call or text message).

Id. at Attachment B.I.[6] Thus, while the Government's aim is to identify or rule out suspects in the crimes that took place at each location, it is asking the Court to give it access to information

[5] "In the experience of CAST, a device's interactions take place on the tower with the strongest and cleanest signal, which is typically the closest tower. Towers are separated into three 120-degree sectors, which together provide 360 degrees of coverage. [Cell-site location information (CSLI)] records include the tower and sector on which a particular transaction took place. Law enforcement can approximate a device's general location based on its use of a specific cell tower and sector for a communication." Aff. ¶ 56.

[6] The Government no longer seeks "the source and destination telephone numbers associated with each communication." Order [6] at 2. But it does acknowledge "the records disclosed in response to a tower-dump request are likely to include the source and destination telephone numbers associated with each communication (including sending and receiving devices outside the area that is specified), regardless of whether this information is included in the request." Aff. ¶ 72. "[T]he wireless providers do not have mechanisms in place to redact certain datapoints" in their own records. *Id.* The Government proposes that CAST redact this information and not share it with the investigative team. *Id.*

about every communication in the covered time and area made by every person, including more detailed location data (beyond the address serviced by a given tower) that the "sector" information will provide. In terms of the temporal scope of the Government's request, each warrant application seeks data for devices connecting to the towers serving the 6 locations for a combined total of 120 minutes. In sum, the Government wants the Court to require the three cellular providers to provide data for a total of 360 minutes—or 6 hours—for every device connecting to any of the towers serving those locations.

II. Analysis

A. The requested warrants will result in a search under the Fourth Amendment.

None of the differences between the earlier applications and these applications impact the Court's previous conclusion that the requested warrants will result in searches for purposes of the Fourth Amendment.[7] For the reasons outlined in its earlier Order [6] at 4–11, the Court concludes that the Government's requested warrants implicate Fourth Amendment concerns.

B. The requested warrants fail to satisfy the Fourth Amendment.

The question is thus whether the Government's warrant applications are "supported by probable cause and particularity." *Smith*, 110 F.4th at 836; *see* U.S. Const. amend. IV ("[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly

[7] The Government observes records "showing the tower and sector used for a communication do not provide an exact location." Aff. ¶ 57. In contrast, "timing advance" records, which it does not seek, provide "more detailed device location information." *Id.* ¶ 57 n.29. That more precise location data may exist does not take these applications outside of the Fourth Amendment. *Carpenter* rejected the argument that "collection of CSLI should be permitted because the data is less precise than GPS information." *Carpenter v. United States*, 585 U.S. 296, 313 (2018) ("[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.' . . . As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas." (citation omitted)).

describing the place to be searched, and the persons or things to be seized."). The Fourth Amendment was adopted in "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Smith*, 110 F.4th at 836 (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)); *see id.* ("'General warrants' are warrants that 'specif[y] only an offense,' leaving 'to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.'" (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981))). To satisfy the Fourth Amendment, "a search or seizure of a person must be supported by probable cause particularized with respect to that person."[8] *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Critically, "[t]his requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Id.* "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Id.*

The problem that persists in the current warrant applications is that if the Court were to issue the warrants, it would be authorizing the Government to search the data for every cellular *device* (including cell phones)[9] of every single individual near the crime scenes without a showing of probable cause as to each individual. *See Ybarra*, 444 U.S. at 92 n.4 ("[A] warrant to

[8] Probable cause for a search "exists when there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute . . . evidence of a crime." *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006). An affidavit supporting a search warrant "must make it apparent, therefore, that there is some nexus between the items to be seized and the criminal activity being investigated." *Id.*

[9] Cellular devices include any device capable of communicating via a cellular network. *See* Aff. ¶ 48 ("By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data."). These could include home alarm systems, smart watches, business point-of-sale systems, and many modern vehicles.

search a place cannot normally be construed to authorize a search of each individual in that place."). And while the applications say that the team investigating the crimes at issue here will not have access to data for any devices that appear at only one of the six locations—presumptive innocent bystanders for whom there is no probable cause—the Government will have obtained that data and searched it to identify and cull relevant devices, i.e., those appearing at more than one of the targeted locations.

As in *Smith*, and as with the previous applications, the tower-dump warrant applications "present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Smith*, 110 F.4th at 837 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). And because they are "general warrants," they are "categorically prohibited by the Fourth Amendment." *Id.* at 838.

III. Conclusion

As explained above and in the Court's previous Order [6], the tower-dump search warrants sought by the Government are materially indistinguishable from the geofence search warrant foreclosed by *Smith*. Accordingly, the Court declines to issue the search warrants.

SO ORDERED AND ADJUDGED this the 27th day of June, 2025.

s/ *Andrew S. Harris*
UNITED STATES MAGISTRATE JUDGE